**U.S. Department of Justice**

*United States Attorney*
*Eastern District of New York*

LJF:AEG
F.#2010R01542

*271 Cadman Plaza East*
*Brooklyn, New York 11201*

August 31, 2010

**By Hand and ECF**

The Honorable Roslynn R. Mauskopf
United States District Judge
Eastern District of New York
225 Cadman Plaza East
Brooklyn, New York 11201

Re: In the Matter of an Application
Misc. Docket No. 10-550

Dear Judge Mauskopf:

On August 16, 2010, the government applied to United States Magistrate Judge James Orenstein, Eastern District of New York, for an order pursuant to 18 U.S.C. § 2703(d) authorizing the disclosure of recorded information identifying the base station towers and sectors that received transmissions from a specified telephone at the beginning and the end of calls or text message transmissions, and the mobile switching center serving the telephone during any calls or text message transmissions, for the period from May 1, 2010 until June 27, 2010 (the "Historical Cell-Site Application" or "Application"). On August 27, 2010, Judge Orenstein denied the application, relying principally on the reasoning of the D.C. Circuit in United States v. Maynard, --- F.3d ----, 2010 WL 3063788, at *19 (D.C. Cir. Aug. 6, 2010), which held that the government must obtain a search warrant based on probable cause shown by affirmation or affidavit before covertly placing a GPS device on the defendant's car and tracking the car's movements for 28 days.[1] Judge Orenstein applied Maynard's reasoning to hold that the government must obtain a warrant to require a cellular telephone service provider to disclose historical cell site data. See In re Application, No. 10-MC-550, Memorandum and Order, Aug. 27, 2010 ("Mem.") at 7.

[1] In doing so Maynard rejected the holdings of United States v. Marquez, 605 F.3d 604 (8th Cir. 2010); United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010); United States v. Garcia, 474 F.3d 994 (7th Cir. 2007). See Maynard, 2010 WL 3063788, at *9.

For the reasons set forth below, Maynard does not govern the Historical Cell-Site Application. Therefore, the government respectfully submits this letter requesting that the Court grant the government's application for historical cell site data.

A disclosure order under 18 U.S.C. § 2703(d) "may be issued by any court that is a court of competent jurisdiction." Therefore, the government may resubmit the Application to Your Honor as miscellaneous judge following its denial by Judge Orenstein.[2] See, e.g., In re Application, 632 F. Supp. 2d 202, 203 (E.D.N.Y. 2008) ("Garaufis").

**A. Background**

The Historical Cell-Site Application seeks an order authorizing the disclosure of recorded information identifying the base station towers and sectors that received transmissions from 347-321-0068, a telephone issued by Sprint Nextel with IMSI Number 316010168456782 subscribed to by Edwin Espinosa, PO Box 54988, Irvine, CA 92619 (the "Subject Telephone"), at the beginning and the end of calls or text message transmissions, and the mobile switching center serving the Subject Telephone during any calls or text message transmissions.[3] Accompanying the government's application were a proposed Order directed to the service provider and a proposed Order of Authorization.

In support of the Historical Cell-Site Application, the government set forth specific and articulable facts showing that

---

[2] Coincidentally the user of the phone targeted by the Application is a defendant in an indicted case before Your Honor, United States v. Tyshawn Augustus, 10-CR-629 (RRM).

[3] The Historical Cell-Site Application requests information regarding "base station towers and sectors." Sprint Nextel, like all other providers to the government's knowledge, retains information regarding only the single antenna tower that received transmissions at the start of a call or text message and the single antenna tower that received transmissions at the end of a call or text message. Accordingly, pursuant to the draft orders provided with the Application, if the Application is granted the government will receive information from Sprint Nextel as to which single tower received the subscriber's transmissions at the beginning, and which single tower received the subscriber's transmissions at the end, of each call or text message. An example of the type of data to be provided is attached as Exhibit A.

there are reasonable grounds to believe that the information sought is relevant and material to an ongoing investigation, the standard set out for such applications in 18 U.S.C. § 2703(d).[4] In particular, the government described its investigation into the possible violation of federal criminal laws, including narcotics offenses in violation of 21 U.S.C. §§ 841, 843, and 846 and firearms offenses in violation of 18 U.S.C. § 924(c). The Historical Cell-Site Application alleged that the user of the Subject Telephone was an individual named Tyshawn Augustus.[5] Based upon the facts described in detail in paragraphs 4 through 14 of the Historical Cell-Site Application, a special agent of the Bureau of Alcohol, Tobacco, Firearms and Explosives concluded that the recorded information sought in the application would be relevant to the investigation of Augustus's commission of the above-mentioned offenses.

**B. Discussion**

**1. Applicable Law**

Pursuant to 18 U.S.C. § 2703(c)(1) and (d), a court may require a provider of electronic communication services to disclose records pertaining to customers to the government if the government offers "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought[] are relevant and material to an ongoing criminal investigation." As Judge Orenstein noted, courts have concluded that this statute reaches historical cell site data. See Mem 4 (citing In re Applications, 509 F. Supp. 2d 76, 79-80 (D. Mass. 2007); Stephen Wm. Smith, 396 F. Supp. 2d 747, 759 n.16 (S.D. Tex. 2005) ("Stephen Wm. Smith"); In re Application, 396 F. Supp. 2d 294, 307 n.10 (E.D.N.Y. 2005)

---

[4] Although not required by Section 2703(d), the government notes as it did in its Application that the facts set forth in that Application are sufficient to establish probable cause that the recorded information sought would constitute evidence of the offenses. See Historical Cell-Site Application ¶ 2 n.1. Judge Orenstein agreed that the facts established probable cause. See Mem. 3 n.3.

[5] The Historical Cell-Site Application notes in paragraph 4, "This investigation has established information indicating that the target [Tyshawn Augustus] is using the SUBJECT TELEPHONE." A confidential informant, who has proven reliable in the past, told the New York City Police Department that Augustus used the Subject Telephone.

(Orenstein, J.)). Congress created the above-mentioned standard that the government must meet to require disclosure to enhance the protection afforded to customer information. See H.R. Rep. No. 103-827(I), at 17 (1994) ("H.R. 4922 includes provisions, which FBI Director Freeh supported in his testimony, that add protections to the exercise of the government's current surveillance authority."); see also id. at 33 ("It is a standard higher than a subpoena, but not a probable cause warrant."). In the absence of the statute, the government would be able to obtain historical cell site data with a subpoena and without any court authorization at all. In addition to concluding that Section 2703 reaches historical cell site data, courts have rejected Fourth Amendment challenges to the government's acquisition of historical cell site data without a search warrant. See United States v. Benford, 2010 WL 1266507, at *3 (N.D. Ind. Mar. 26, 2010) (denying suppression of historical cell-site data); United States v. Jenious, No. 09-CR-097, Slip Op. at 6-11 (E.D. Wis. Aug. 28, 2009) (attached hereto as Exhibit B) (same); United States v. Suarez-Blanca, 2008 WL 4200156, at *8-*11 (N.D. Ga. Mar. 26, 2008) (same); In re Application, 405 F. Supp. 2d 435, 449-50 (S.D.N.Y. 2005) ("Gorenstein") (granting application for 2703(d) order for historical cell-site data); Mitchell v. State, 25 So.3d 632, 635 (Fla. Dist. Ct. App. 2009) (rejecting challenge to trial court's admission of historical cell-site data).[6]

**2. United States v. Maynard**

In Maynard, the D.C. Circuit overturned the defendant's conviction because the police did not obtain a warrant before covertly placing a GPS device on the defendant's car and tracking the car's movements for 28 days. See Maynard, 2010 WL 3063788, at *19. The court held that the use of the GPS device was a search for constitutional purposes because it defeated the defendant's reasonable expectation of privacy. See id. at *7. First, the court reasoned that "the whole of a person's movements over the course of a month is not actually exposed to the public

[6] The government is aware of two courts that have held that the government must demonstrate probable cause to obtain historical cell-site data. See In re Application, 534 F. Supp. 2d 585, 585-86 (W.D. Pa. 2008) ("Lenihan"), aff'd, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008); In re United States, 2006 WL 1876847, at *1 (N.D. Ind. July 5, 2006). The government's appeal of the decision in the Western District of Pennsylvania is pending. See In re Application, No. 08-4227 (3d Cir. argument held Feb. 12, 2010) (docket sheet available on PACER).

because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil." Id. at *12.[7] Second, the court reasoned that "the whole of a person's movements over the course of a month" is not constructively exposed to the public through the exposure of each individual movement because "the whole reveals far more than the individual movements it comprises." Id. at *13. Finally, the court reasoned that the defendant's expectation of privacy in his movements over the course of a month was reasonable because "prolonged GPS monitoring reveals an intimate picture of the subject's life that he expects no one to have - short perhaps of his spouse." Id. at *14. As a result, the court held that the government needed to obtain a warrant before applying the GPS device to the defendant's car. See id. at *16.

**3. The Reasoning of Maynard Does Not Apply to Historical Cell-Site Data**

The reasoning of Maynard does not apply to historical cell-site data. There are at least four crucial differences between the data at issue in Maynard and that sought here.

First, in Maynard, law enforcement officers caused data to be created that would not otherwise have existed. By contrast, in this case the government seeks access to data that a third party already created, collected and maintained in the ordinary course of its business.

Second, the Maynard law enforcement officers covertly placed equipment upon the defendant's property to obtain location data. Here, the location data originated from equipment – a cell phone – that a person knowingly and voluntarily used and which equipment transmitted data as part of its normal operation.

Third, in Maynard the GPS device provided data to the government 24 hours a day, allowing law enforcement officers to track the defendant in real time. Here, cell-site data exists only for the moments in time during which the phone was engaged in a call or text message transmission, and it is being sought only retrospectively.

---

[7] For the same reason, the court concluded that the propriety of warrantless GPS tracking for 28 days was not governed by United States v. Knotts, 460 U.S. 276, 277, 285 (1983), which approved warrantless use of a beeper device to track a vehicle during a single trip.

Fourth, Maynard involved the most precise of all location information: GPS data. In this case, the government requests cell-site data, which is much less precise. Notably, cell-site data is especially imprecise in an area as densely inhabited as New York City, where many buildings - and the numerous residences and businesses within those buildings - are likely to be served by a single base station tower and mobile switching center.

Because of these differences, the reasoning of Maynard does not apply to the government's request for disclosure of historical cell-site data. As noted above, the court in Maynard relied on three bases to conclude that the GPS device required a warrant: the whole of a person's movements over the course of a month (1) "is not actually exposed to the public because the likelihood a stranger would observe all those movements . . . is essentially nil," id. at *12, (2) is not constructively exposed to the public through the exposure of each individual movement because "the whole reveals far more than the individual movements it comprises," id. at *13, and (3) "reveals an intimate picture of the subject's life that he expects no one to have - short perhaps of his spouse," id. at *14. None of these analyses applies to historical cell-site data. The entire collection of data the government seeks has already been "actually exposed" to a third party: Sprint Nextel. The user of the Subject Telephone knows or should know that every time he places or receives a call Sprint Nextel is advised of the cell tower being used, because the user knows that Sprint Nextel may later charge him for its services based in part on his location. (See Nationwide Sprint PCS Network, available at http://www.sprintpcs.com/pages/exception_map.html (last visited Aug. 29, 2010) (attached hereto as Exhibit C).) Furthermore, the entire collection of data does not reveal far more than the individual pieces of data it contains, nor does it reveal an intimate portrait of the user's life. The data reveals the general area where the user was when the user placed or received calls. It does not indicate where the user was within a particular building, and indeed likely would not even indicate what building the user was in or near. Moreover, the data does not include any information at all about where the user was during the vast majority of the day when he was not using the Subject Telephone. For all of these reasons, the user has no reasonable expectation of privacy in the historical cell site data. The concerns that led the Maynard court to hold that the government must obtain a warrant before applying a GPS device to

an individual's car do not apply to the government's application here.[8]

Judge Orenstein rejected the above arguments. First, he reasoned that the fact that the government sought historical rather than prospective data did not affect whether Augustus had a reasonable expectation of privacy in the data. See Mem. 12-13. As Judge Orenstein noted elsewhere in his Memorandum and Order, however, prospective data can serve at least one important purpose for the government that historical data cannot: prospective data "may ease the task of commencing or continuing physical surveillance." Mem. 23 n.18. As a result, the government in Maynard could use the data it obtained to carry out additional investigation to create a far more "intimate picture of the subject's life," Maynard, 2010 WL 3063788, at *14, than would be available to the government here. The distinction between historical and prospective data thus directly impacts the Maynard court's rationale and weighs against applying that rationale to the Historical Cell Site Application.

Judge Orenstein also concluded that the fact that Maynard addressed GPS information while the Historical Cell Site Application addresses cell site information should not prevent Maynard's reasoning from applying here. See Mem. 19-23. Judge Orenstein reasoned that, while cell site information may not reveal a user's precise location, neither does GPS tracking: "GPS tracking by itself does not necessarily reveal a subject's '[r]epeated visits to church, a gym, a bar, or a bookie[.]'" Mem. 20 (quoting Maynard, 2010 WL 3063788, at *13; alterations in Mem.). Judge Orenstein also noted that, if cell site information does not reveal the user's location when he or she is not using the phone, neither did the GPS data in Maynard reveal where the defendant was when he was not driving. Mem. 21, 28-29. The latter point ignores that the GPS device in Maynard transmitted data 24 hours a day, informing the government at least where the car was at all times; the historical cell site information sought here would provide no information about the location of the user or the phone except when calls are made or text messages are sent or received. In any event, both points demonstrate only that

---

[8] In the government's view Maynard was wrongly decided. See generally United States v. Marquez, 605 F.3d 604 (8th Cir. 2010); United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010); United States v. Garcia, 474 F.3d 994 (7th Cir. 2007); United States v. Jesus-Nunez, 2010 WL 2991229 (M.D. Pa. July 27, 2010). The Court need not evaluate Maynard on its own merits, however, to rule on this application.

Maynard is not persuasive.[9] They do not suggest that this Court should extend Maynard's unpersuasive reasoning to the government's application for cell site information.

Judge Orenstein also noted that 18 U.S.C. § 2703 does not distinguish among various forms of historical location data and reasoned that "any argument predicated on the relative precision of a given tracking method does nothing to validate the constitutionality of the [statute's] standard of 'specific and articulable facts' in the context of location tracking." Mem. 19 n.13. But this Court need not and should not evaluate the facial constitutionality of the statute in all of its applications. See Sibron v. New York, 392 U.S. 40, 62 (1968) ("Our constitutional inquiry would not be furthered here by an attempt to pronounce judgment on the words of the statute [authorizing certain warrantless seizures]. We must confine our review instead to the reasonableness of the searches and seizures which underlie these two convictions."). Similarly, Judge Orenstein observed that if the fact that Sprint Nextel maintains cell site data with respect to only one tower at each end of calls and text messages, and therefore that the Historical Cell Site Application seeks relatively imprecise data, is determinative, "then all future applications for [cell site data] must necessarily get bogged down in an inquiry into the precise record-keeping practices currently followed by the relevant service provider." Mem. 19 n.13; see also Mem. 22 n.16 (concluding government's argument concerning relative precision of cell site data and GPS data "assures virtually instant obsolescence to a decision here in the government's favor" because cell site data may be more precise in the future). In the government's view Maynard is inapposite for all of the reasons discussed herein, such that the number of towers from which data is sought is not alone determinative. But to the extent that detail or any other is relevant to the

---

[9] Indeed, the latter point undermines the very premise of Maynard, that it was addressing the scenario upon which the Supreme Court reserved decision in Knotts. Maynard noted that Knotts rejected the defendant's argument that approving the GPS tracking used in that case would permit "'twenty-four hour surveillance of any citizen of this country . . . without judicial knowledge or supervision,'" because if such law enforcement practices were eventually employed, "there will be time enough then to determine whether different constitutional principles may be applicable." Knotts, 460 U.S. at 283 (quoted at Maynard, 2010 WL 3063788, at *8). As Judge Orenstein noted, however, the GPS monitoring in Maynard did not constitute 24-hour surveillance of the defendant.

analysis, fact-specific results are not objectionable. Cf. United States v. Gori, 230 F.3d 44, 55 (2d Cir. 2000) ("The reasonableness under the Fourth Amendment of any Terry stop is by definition fact-specific.").

Judge Orenstein also reasoned that, "in seeking to distinguish Maynard on the ground that [cell site data] is not very precise, the government proves too much," because, after all, the government is seeking the data for a reason. Mem. 22. It is true that, as noted in the Historical Cell Site Application, the government believes the data is relevant to its investigation because it provides some information about the target's location. But maintaining that belief and observing that cell site data is less precise than GPS data is not "hav[ing] it both ways," as Judge Orenstein suggests. Mem. 23. It is simply recognizing historical cell site data for whatever value it has, no more and no less. Similarly, telephone toll records are less detailed than the content of telephone calls, but toll records nonetheless can further a government investigation and can be obtained without a search warrant. Judge Orenstein's rationale suggests that all useful evidence is protected by the Fourth Amendment, abandoning the well-established rule that the protection applies only when an individual has a reasonable expectation of privacy. See United States v. Hayes, 551 F.3d 138, 143 (2d Cir. 2008) ("A Fourth Amendment 'search,' however, does not occur unless the search invades an object or area where one has a subjective expectation of privacy that society is prepared to accept as objectively reasonable.") (citing Illinois v. Caballes, 543 U.S. 405, 408 (2005)).

**4. The Government Is Not Required to Demonstrate Probable Cause to Obtain Historical Cell-Site Data**

Finally, Judge Orenstein characterized as "meaningless" the fact that in Maynard the government covertly placed equipment on the defendant's property to obtain GPS data, while here the government seeks data from a cell phone that a person knowingly and voluntarily used, and that transmitted data to Sprint Nextel as part of its normal operation. See Mem. 28. Under the established principles of United States v. Miller, 425 U.S. 435 (1976), and Smith v. Maryland, 442 U.S. 735 (1979), however, there is no reasonable expectation of privacy in historical cell-site data that a cell phone user voluntarily causes to be transmitted to a cell phone provider. Thus, Maynard is inapposite and the Fourth Amendment does not limit disclosure of historical cell-site data pursuant to 2703(d) orders.

**a. United States v. Miller and Smith v. Maryland**

The historical cell-site data at issue is not in the hands of the cell phone user at all, but rather in the business records of a third party – Sprint Nextel. The Supreme Court has held that a customer has no privacy interest in business records of this kind. Addressing a Fourth Amendment challenge to a third party subpoena for bank records, the Court held in United States v. Miller, 425 U.S. 435 (1976), that the bank's records "are not respondent's 'private papers'" but are "the business records of the banks" in which a customer "can assert neither ownership nor possession." Miller, 425 U.S. at 440; see also SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984) ("when a person communicates information to a third party . . . he cannot object [on the basis of the Fourth Amendment] if the third party conveys that information or records thereof to law enforcement authorities"). Thus, an individual has no Fourth Amendment-protected privacy interest in business records, such as cell-site usage data, that are kept, maintained and used by a cell phone company in the normal course of business. If anything, the privacy interest in cell-site data is even less than the privacy interest in bank records. The location and identity of the cell phone tower handling a customer's call is generated internally by the phone company and is not, therefore, typically known by the customer. A customer's Fourth Amendment rights are not violated when the phone company reveals to the government its own records that were never in the possession of the customer.

Further, even if cell-site data were disclosed by the subscriber himself to the telephone company, the subscriber would have no reasonable expectation of privacy in the data pursuant to Smith v. Maryland. In Smith, the Court held both that telephone users do not likely have an actual expectation of privacy in dialed telephone numbers and also that any expectation they do have is not reasonable. See Smith, 442 U.S. at 742-44. The Court's reasoning applies equally to cell-site data. First, the Court stated: "we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." Id. at 742. Similarly, cell phone users understand that they must send a radio signal, which is received by a cell phone company's antenna in order to route their call to its intended recipient. (Indeed, cell phone users are intimately familiar with the relationship between call quality and radio signal strength, as typically indicated by a series of bars on their phones' displays.)

Second, under the reasoning of Smith, any subjective expectation of privacy in cell-site data is unreasonable. In Smith, the Court explicitly held that, "even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not one that society is prepared to recognize as reasonable." Id. at 743 (internal quotation marks omitted). The Court noted that "[t]his Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Id. at 743-44. In Smith, the user "voluntarily conveyed numerical information to the telephone company" and thereby "assumed the risk that the company would reveal to the police the numbers he dialed." Id. at 744. When a cell phone user transmits a signal to a cell tower for his call to be connected, he similarly assumes the risk that the cell phone provider will create its own internal record of which of its towers handles the call. Thus, it makes no difference if some users have never thought about how their cell phones work; a cell phone user can have no expectation of privacy in cell-site data.[10]

Miller and Smith illustrate the fundamental principle that the Fourth Amendment does not require the government to obtain a search warrant before asking third parties questions about suspects. That is why the constitutional analysis of the government's covertly placing equipment on the defendant's property to obtain GPS data in Maynard cannot be applied to the government's attempt here to obtain from Sprint Nextel data from a cell phone that a person knowingly and voluntarily used, and that transmitted data to Sprint Nextel as part of its normal operation. Other courts have held these constitutional principles directly applicable to cell site data and rejected Fourth Amendment challenges to obtaining it. See Benford, 2010 WL 1266507, at *3; Jenious, Slip Op. at 6-11 (same); Suarez-Blanca, 2008 WL 4200156, at *8-*11 (same); Gorenstein, 405 F. Supp. 2d at 449-50 (granting application for 2703(d) order for historical cell-site data); Mitchell, 25 So.3d at 635 (rejecting challenge to trial court's admission of historical cell-site

---

[10] Judge Orenstein noted that "a mobile telephone user knowingly and voluntarily speaks into her device, which then broadcasts the contents of her communications as part of its normal operations. That fact plainly does not shield the contents of the broadcast communications from the protection of the Fourth Amendment's warrant requirement." Mem. 28. Such reasoning, however, would reject the result in Smith.

data); but see Lenihan, 534 F. Supp. 2d at 585-86; In re United States, 2006 WL 1876847, at *1.

A different result would cast doubt on a wide array of routine, judicially approved government investigative techniques. For example, if the government arrests a defendant and finds credit cards in his wallet, it may use a subpoena to ask the credit card companies where the cards have been used. See United States v. Phibbs, 999 F.2d 1053, 1076-77 (6th Cir. 1993) (rejecting Fourth Amendment-protected privacy right in credit card statements). Similarly, if the government finds the defendant's subway farecard, or learns through surveillance that a suspect uses an automated system to pay highway tolls, it could almost certainly obtain subway and highway toll records with a subpoena.

Judge Orenstein concluded that Miller and Smith did not govern historical cell site data, relying on Warshak v. United States, 490 F.3d 455 (6th Cir. 2007), vacated on other grounds, 532 F.3d 521 (6th Cir. 2008) (en banc); Stephen Wm. Smith, 396 F. Supp. 2d 747, and the Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, 113 Stat. 1286 (Oct. 26, 1999). See Mem. 13-19. These authorities, however, do not support Judge Orenstein's ruling.

**b. Warshak v. United States**

In Warshak, the court held that the government must obtain a search warrant supported by probable cause to require an internet service provider ("ISP") to disclose the contents of a user's email. See Warshak, 490 F.3d at 473. The court reasoned,

> The combined precedents of [Katz v. United States, 389 U.S. 347 (1967),] and Smith . . . recognize a heightened protection for the content of the communications. Like telephone conversations, simply because the phone company or the ISP could access the content of e-mails and phone calls, the privacy expectation in the content of either is not diminished, because there is a societal expectation that the ISP or the phone company will not do so as a matter of course.

See id. at 471 (emphasis in original) (quoted in part at Mem. 15). Judge Orenstein concluded that Warshak "explains why a person may reasonably maintain an expectation of privacy in

information about herself that she knows to be held by others." Mem. 14. Warshak, however, is not instructive here.

First, of course, the contents of email and telephone calls are undeniably more private than historical cell site data. Even if it is correct that an expectation of privacy in email or telephone content is reasonable, that says little about whether such an expectation concerning cell site data is reasonable. Second, the Warshak court's reasoning that an email user retains an expectation of privacy in email because society expects that, despite its ability to do so, the ISP will not in fact read his or her email does not apply to cell site data. Cell phone providers use the fact of a user's connection to a particular base station tower for customer billing based on where the phone is used.[11] See also U.S. Telecomm. Ass'n v. FCC, 227 F.3d 450, 463 (D.C. Cir. 2000) (signals sent from cell phones to cell sites "are necessary to achieve communications between the caller and the party he or she is calling" (quoting brief of FCC)). The importance of this distinction is highlighted by Judge Orenstein's inaccurate summary of Warshak's "fundamental rationale" as being "that a user of communications services can have a very reasonable expectation that the service provider's necessary access to certain otherwise private information need not expose such information to the world at large." Mem. 16 n.11 (emphasis added). The crucial fact in Warshak was that society in general and the email user in particular expect that an ISP in practice will not access the content of the user's email. See Warshak, 490 F.3d at 471. That is the basis on which the Warshak court distinguished Phibbs, which approved the use of mere subpoenas to obtain credit card records. See id. at 469. If the ISP did in fact access the content, the case would be more closely analogous to the telephone numbers dialed in Smith, and the Warshak court would likely have reached a different result. Because cell site data is in fact accessed by Sprint Nextel, the reasoning of Warshak does not apply here.

**c. Stephen Wm. Smith**

In Stephen Wm. Smith, 396 F. Supp. 2d at 748, the court granted the government's application for historical cell site

---

[11] Judge Orenstein apparently doubted that today billing ever or often depends on a user's location. See Mem. 24. In fact, however, even now some Sprint Nextel subscribers are charged additional fees when – because of their location when using the phone – they are outside the company's network. See Nationwide Sprint PCS Network.

data but denied its application for prospective cell site data. The court concluded that the disclosure of prospective cell site data converted a cell phone into a tracking device and therefore that, pursuant to 18 U.S.C. § 3117, the government must employ a warrant supported by probable cause to obtain such data. See id. at 753-57. Thus the court's discussion, quoted by Judge Orenstein, of reasonable expectations of privacy in relation to "cell phone tracking," id. at 756 (quoted at Mem. 16), concerns data significantly different from that at issue here.

In addition to being prospective, the data at issue in Stephen Wm. Smith – at least in that court's view – was substantially more precise than the data at issue here. The court noted that, "By a process of triangulation from various cell towers, law enforcement is able to track the movements of the target phone, and hence locate a suspect using that phone." Id. at 751. As noted above, however, here the government seeks only data revealing which single tower received the subscriber's transmissions at the beginning, and which single tower received the subscriber's transmissions at the end, of each call or text message. Such data does not permit the triangulation that concerned the court in Stephen Wm. Smith. See Garaufis, 632 F. Supp. 2d at 208 ("the Government is seeking only information identifying the one antenna tower . . . . Such information, unlike the information revealed by triangulation or by more advanced communications devices . . . is not precise enough to enable tracking of a telephone's movements within a home." (citation omitted)).[12]

---

[12] Judge Orenstein cites Lenihan, 534 F. Supp. 2d at 602, for the proposition that, "[a]s of February 2008, [cell site data] from multiple towers could reveal the location of a cell phone to within approximately 50 feet, and information from a single tower to within a few hundred feet." Mem. 21 n.14. This assertion is incorrect. In fact, "the actual location of the caller can be miles distant from the" cell site or base station receiving a call. In re Alltel Corp., 22 FCC Rcd. 16432, 16436 n.32 (Aug. 30, 2007). The assertion in Lenihan appears to be derived from Kevin McLaughlin, Note, The Fourth Amendment and Cell Phone Location Tracking: Where Are We?, 29 Hastings Comm. & Ent. L.J. 421 (2007) (cited at Lenihan, 534 F. Supp. 2d at 590 n.17). McLaughlin, 29 Hastings Comm. & Ent. L.J. at 426-27 n.29, in turn cites Gorenstein, 405 F. Supp. 2d at 437. That decision, however, says merely that in Lower Manhattan cell phone towers "may be anywhere from several hundred feet to as many as 2000 feet or more apart." Id. Indeed, Gorenstein notes that, as is the case here, "at any given moment, data is provided only as to

Moreover, the court in Stephen Wm. Smith, 396 F. Supp. 2d at 748, apparently understood the application before it to seek all cell site data created while the cell phone was turned on. The court noted, "It should be emphasized that cell site data transmitted during the registration process are not dialed or otherwise controlled by the cellular telephone user. This registration process automatically occurs even while the cell phone is idle." Id. In the passage relied upon by Judge Orenstein, the Stephen Wm. Smith court reasoned, "Unlike dialed telephone numbers, cell site data is not 'voluntarily conveyed' by the user to the phone company. As we have seen, it is transmitted automatically during the registration process, entirely independent of the user's input, control, or knowledge." Id. at 756-57 (quoted at Mem. 16). Here, in contrast, the government seeks only data that was recorded at the start and end of calls and text messages. This distinction alone renders Stephen Wm. Smith inapposite, because a central aspect of Stephen Wm. Smith's reasoning does not apply. The data here is no different from that at issue in Smith v. Maryland.[13]

**d. The Wireless Communications and Public Safety Act of 1999**

Following Stephen Wm. Smith, 396 F. Supp. 2d at 757, Judge Orenstein also relied upon the Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, 113 Stat. 1286

---

a single cell tower with which the cell phone is communicating. Thus, no data is provided that could be 'triangulated' to permit the precise location of the cell phone user." Id. at 438. Discussions of data from multiple towers in Judge Orenstein's Memorandum and Order and in Stephen Wm. Smith are irrelevant to the Historical Cell Site Application.

[13] Judge Orenstein asserts that – unlike placing a call or sending a text message – receiving a call or text message occurs "without any voluntary action" by the cell phone user. Mem. 21 n.15. In fact, a cell phone user must voluntarily accept an incoming call, either by opening the phone or by pressing a button. Cell site data is not recorded for calls that are answered by voicemail rather than by the cell phone user. Though it is true that a cell phone user takes no active step to receive a particular text message, he or she voluntarily signed up for text message service and would rarely if ever receive a text message without voluntarily making known to others that he or she used that form of communication, either by sending text messages or otherwise.

(Oct. 26, 1999) (the "Act"), to conclude that cell phone users have a reasonable expectation of privacy in cell site data. See Mem. 17-18. This legislation, however, supports the opposite conclusion. The Act required that cell phone service providers adopt 911 as the number to be dialed to reach emergency services. See Act § 3(a). It also permitted providers to disclose "call location information" to emergency services. Act § 5(1); see also S. Rep. No. 106-138, at 7 (1999) ("This section requires the provision of call location information to emergency service personnel and data management services solely for the purpose of assisting in the delivery of emergency services."). It did so by amending 47 U.S.C. § 222, which requires telecommunications companies to "use, disclose, or permit access to" customer information only in their provision of the service from which the data was derived, "[e]xcept as required by law or with the approval of the customer" and for certain other purposes. 47 U.S.C. §§ 222(c)(1), (d). The Act added the disclosure of "call location information" to emergency services to the list of other purposes for which telecommunications companies may disclose customer information. Act § 5(1).

The Act also added a new provision clarifying the pre-existing "approval of the customer" exception to the bar on use and disclosure of customer information. The new provision – cited by Stephen Wm. Smith, 396 F. Supp. 2d at 757, and Judge Orenstein, see Mem. 17-18 – declares that, "without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to . . . call location information." Act § 5(2) (codified at 47 U.S.C. § 222(f)). The court in Stephen Wm. Smith and Judge Orenstein viewed this new provision as demonstrating a congressional recognition and codification of a reasonable expectation of privacy in cell site information. They are mistaken. First, the phrase "except as required by law" of course includes an exception for criminal legal process, see Parastino v. Conestoga Tel. & Tel. Co., 1999 WL 636664, at *1-2 (E.D. Pa. Aug. 18, 1999) (dismissing lawsuit alleging violation of 47 U.S.C. § 222 because disclosure made pursuant to state court subpoena in criminal investigation), so the original language of the statute – left untouched by the amendment – contemplates disclosure to government investigators. Moreover, the amendment was enacted as part of an Act permitting the disclosure of call location information to government personnel. If anything, the Act as a whole demonstrates that it is objectively unreasonable for anyone to maintain an expectation of

privacy – at least vis-a-vis the government – in the data created by the use of a cell phone.[14]

In any event, statutory rights do not necessarily illustrate the scope of an individual's reasonable expectation of privacy. See Orin Kerr, Fourth Amendment Stunner: Judge Rules That Cell-Site Data Protected By Fourth Amendment Warrant Requirement, The Volokh Conspiracy (Aug. 31, 2010, 2:46 a.m.), http://volokh.com/2010/08/31/fourth-amendment-stunner-judge-rules-that-cell-site-data-protected-by-fourth-amendment-warrant-requirement/ (discussing City of Ontario v. Quon, 130 S. Ct. 2619, 2632 (2010) (citing Virginia v. Moore, 553 U.S. 164, 176 (2008) ("We conclude that warrantless arrests for crimes committed in the presence of an arresting officer are reasonable under the Constitution, and that while States are free to regulate such arrests however they desire, state restrictions do not alter the Fourth Amendment's protections."); California v. Greenwood, 486 U.S. 35, 43 (1988) ("We reject respondent Greenwood's alternative argument for affirmance: that his expectation of privacy in his garbage should be deemed reasonable as a matter of federal constitutional law because the warrantless search and seizure of his garbage was impermissible as a matter of California law."))). For all of the reasons discussed herein, even if the Act implied an expectation by Congress of privacy in call location information against government investigation of crime – which it does not – that expectation would not be reasonable under the Fourth Amendment.

**e. Sprint Nextel's Privacy Policy**

Judge Orenstein also noted "the growing availability and popularity of commercial applications that allow a mobile

---

[14] The congressman who added the provision cited by Stephen Wm. Smith and Judge Orenstein to the Act intended it to prevent cell phone providers from selling location information. See 145 Cong. Rec. H9858-01, H9860 (daily ed. Oct. 12, 1999) (statement of Rep. Markey) ("They should have to come to you and say we want to sell this information to anyone who wants to buy it as to where you are going."). Two other congressmen supported the provision as protecting such information from disclosure to the government, see id. (statement of Rep. Tauzin); id. at H9862 (statement of Rep. Green), and a third favored both rationales for the provision, see id. at H9863 (statement of Rep. Bliley). As noted above, in light of the overall purposes of the Act, viewing the provision as limiting the government's access to location information is nonsensical.

telephone user to affirmatively broadcast her location" and asserted that "a growing awareness of the possibility of location tracking of mobile phones has also produced a growing expectation that such tracking can and should be controlled." Mem. 24-25 (emphasis in original). Judge Orenstein noted that the privacy policies of Verizon Wireless, AT&T, Google and a cell phone application called "foursquare" attempt to reassure customers about their use of location information. See Mem. 25-26.

In contrast, however, the privacy policy of Sprint Nextel, the company at issue here, provides no such reassurance. The policy notes, "We automatically receive certain types of information whenever you use our Services. . . . For example, we collect . . . information about . . . your location." (Sprint Nextel Privacy Policy, available at http://www.sprint.com/legal/privacy.html?INTNAV=ATG:FT:Privacy (last visited Aug. 29, 2010), attached hereto as Exhibit D). The policy also states, "When you leave our network you may also use mobile roaming services provided by third parties. Your use of such services and applications may result in these third parties collecting your personal information and obtaining information from Sprint, including location information (when applicable)." Finally, the policy notes, "We may access, monitor, use or disclose your personal information or communications to do things like: comply with the law or respond to lawful requests or legal process . . . ." To the extent that the cell phone provider's privacy policy is relevant, Sprint Nextel's policy – the only one conceivably relevant here – substantially undermines the reasonableness of any expectation of privacy by its customers.

## Conclusion

For these reasons, the government respectfully requests that its request for historical cell-site information be granted based on its offering of specific and articulable facts showing that there are reasonable grounds to believe that the information sought is relevant and material to an ongoing criminal investigation.

Respectfully submitted,

LORETTA E. LYNCH
United States Attorney

By: /s/
Andrew E. Goldsmith
Assistant U.S. Attorney
(718) 254-6498